

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

In the Matter of the Search of

The residence at 1629 South 37th Street, Milwaukee, Wisconsin, is more particularly described as follows: A two-story residence, the lower half of the residence contains white siding with maroon trim and the upper half contains maroon siding with white trim. The address "1629" is affixed to the mail box near the front door of the residence. In addition, there is a detached two-car garage with light colored siding and a red garage door.

**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**

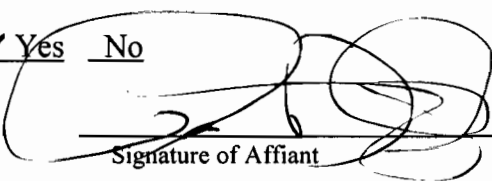
CASE NUMBER: 09-M-504

I, Jason B. Fleming, being duly sworn depose and say: I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that on the property known as 1629 South 37th Street, Milwaukee, Wisconsin, in the Eastern District of Wisconsin, there is not now concealed certain property, namely: evidence of violation of Title 18, United States Code, Section 2252(a)(4)(B) (possession of child pornography), as set forth in Attachment A.

The facts to support a finding of Probable Cause are as follows:

See the attached affidavit.

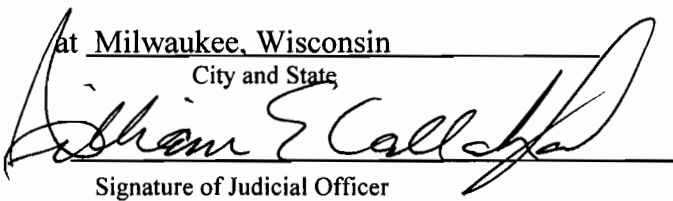
Continued on the attached sheet and made a part hereof. ☒ Yes ☐ No


Signature of Affiant

Sworn to before me, and subscribed in my presence

August 20, 2009 at 3:10 PM
Date and time issued

William E. Callahan, Jr., U.S. Magistrate Judge
Name & Title of Judicial Officer


at Milwaukee, Wisconsin
City and State

Signature of Judicial Officer

Affidavit In Support Of Search Warrant For The Residential Property Located At:

1629 South 37th Street
Milwaukee, Wisconsin

I, Jason B. Pleming, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. I have been employed with the FBI as a Special Agent since January of 2007. I am currently assigned to the Milwaukee Division Cyber Crimes Task Force (CCTF). I am charged with conducting investigations of violations of federal law including the receipt, possession, distribution, and production of child pornography. I have gained experience in the conduct of such investigations through prior investigations, formal training, and in consultation with other members of the CCTF regarding these matters. As a Federal Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.
2. This affidavit is being submitted in support of an Application for a Search Warrant for the residence located at 1629 South 37th Street Milwaukee, Wisconsin, for evidence of violations of Title 18, United States Code (U.S.C.), § 2252A, entitled "Certain activities relating to material constituting or containing child pornography."
3. Based upon the information summarized in this application, I have reason to believe that evidence of such violations may be present at the residence located at 1629 South 37th Street Milwaukee, Wisconsin.
4. The information supplied in this affidavit is based upon my investigation, information provided by and investigation conducted by other law enforcement personnel in this matter to date. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not set forth every fact of this investigation.

Applicable Law

5. This investigation concerns alleged violations of United States Code, §2252A, entitled, "Certain activities relating to material constituting or containing child pornography," which provides in part:
- a. any person who -
 - i. knowingly mails or transports or ships, in interstate or foreign commerce by any means, including by computer, any child pornography;
 - ii. knowingly receives or distributes -
 - (1) any child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer; or
 - (2) any material that contains child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any mean, including by computer;
 - iii. knowingly -
 - (1) re produces any child pornography for distribution through the mails, or in interstate or foreign commerce by any means, including by computer; or
 - (2) advertises, promotes, presents, distributes, or solicits through the mails, or in interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains -
 - (a) an obscene visual depiction of a minor engaging in sexually

explicit conduct; or

- (b) a visual depiction of an actual minor engaging in sexually explicit conduct;

iv. ...

v. either -

(1) ...

- (2) knowingly possesses any book, magazine, periodical, film videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer; or

vi. knowingly distributes, offers, sends, or provides to a minor any visual depiction, including any photograph, film, video, picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, where such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct -

- (1) that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer;
- (2) that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer; or
- (3) which distribution, offer, sending, or provision is accomplished

using the mails or by transmitting or causing to be transmitted any wire communication in interstate or foreign commerce, including by computer,

- for purposes of inducing or persuading a minor to participate in any activity that is illegal.

6. Per Title 18, U.S.C., § 2256(1), the term "minor" means any person under the age of eighteen years.
7. Per Title 18, U.S.C., § 2256(2), term "sexually explicit conduct" means actual or simulated:
 - a. sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; or
 - b. bestiality; or
 - c. masturbation; or
 - d. sadistic or masochistic abuse; or
 - e. the lascivious exhibition of the genitals or pubic area of any person.
8. Per Title 18, U.S.C., § 2256(8), the term "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where -
 - a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
 - b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or,

- c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Definitions of Technical Terms Pertaining to Computers

9. The "Internet" is a collection of computers that are connected to one another via high-speed data links and telephone lines for the purpose of sharing information and services. Connections between Internet computers may exist across state and international borders and information sent between computers connected to the Internet frequently cross state and international borders, even if those computers are located in the same state. In order to access the Internet, an individual computer must subscribe to an access provider, which operates a host computer system with direct access to the Internet.
10. Internet Service Providers (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email communication, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name - a user name or screen name, an email address, an email mailbox, and a personal password selected by the subscriber. By using a computer connected to a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of

whether those subscribers are individuals or entities). These records may include subscriber and billing information, account information (often times in the form of log files), email communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format.

11. Every computer or device on the Internet is referenced by a unique Internet Protocol (IP) address while the computer is connected to the Internet. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IP address is 192.168.10.101. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next dial-up customer. On the other hand, some ISP's, including most cable providers, employ static IP addressing, that is a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a

specific computer. It is also possible that a subscriber may retain an IP address for a medium period of time then be reassigned another IP address from the ISP.

Background on the Use of Computers for Child Exploitation

12. In my experience, the primary manner in which child pornography is produced, distributed, and possessed is through the use of computers. Pornographers produce both still and moving images directly from common video or digital cameras attached to a computer. Producers of child pornography often use a device known as a scanner to transfer photographs into a computer readable format, and then either send the images directly through the Internet or copy the images onto a disk and send them through the U.S. mails. Many digital cameras can be connected directly to a computer and through the use of various software programs, photographs and videos can be transferred directly to a computer, can be transferred to another computer via the Internet, and can be stored directly onto a computer.
13. Each time an individual views an online digital image, that image, or remnants of that image, are automatically stored on the hard-drive of the computer used to view the image. Once an individual opens an image of child pornography on his computer or accesses such an image through the Internet, that image is saved in the computers "cache." This allows investigators to review a history of the images opened/accessed by the user of the computer long after the image has been opened or accessed.
14. Digital information can also be retained unintentionally, e.g. traces of the path of an electronic communication may be automatically stored in many places (e.g. temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence

suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files, which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data. In fact, I am aware that computer files or remnants of files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Even when the files have been deleted, they can be recovered months or years later using readily available forensic tools. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

15. Individuals who possess, receive, transfer, and distribute child pornography use communication devices known as a modem or cable connections that allow any computer to connect to another computer by telephone line, cable, or wireless service. By connection to an Internet service provider, electronic contact can be made to millions of computers around the world. Internet service providers are sometimes commercial concerns, which allow subscribers to dial local numbers and connect to a network, which is connected to their host systems. "Hotmail," for example, is an anonymous and free email service based in California. These Internet service providers allow electronic mail service between subscribers, and usually between their own subscribers and those of other networks. Once one has subscribed to an Internet service provider, it costs nothing

to send or receive image files. Further, each image is a digital duplicate of the computer original, and a child pornography distributor's collection is thus not diminished by distributing the pornography to others via computer. This open and anonymous communication allows the user to locate others of similar inclination and still maintain anonymity. Once contact is established, it is then possible to send text messages and graphic images to others. These communications can be quick, relatively secure, and as anonymous as desired.

16. The ability to store images in digital form makes the computer an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown exponentially within the last several years. Hard drives with a capacity of one hundred gigabytes are not uncommon, and these drives can store thousands of images at very high resolution.
17. Images can be electronically mailed to anyone with access to a computer and modem, and they can be downloaded onto computers, computer discs, or CD-ROM's for ease of storage, duplication, and distribution. With the proliferation of commercial services providing Internet service, computer transfer and digital copying is the preferred method of distributing child pornography.
18. The capacity of computers, and the ease of access and relative anonymity afforded to computer users, permits individuals with an interest in child pornography to amass large collections of such materials.
19. In my experience, individuals involved in the collection and distribution of child pornography often categorize the images in their collections, constantly seek new materials to add to their collections, and maintain their collections for many years. I have been involved in the execution of a search warrants involving child pornography for

residences in which items seized revealed a collection of child pornography that dated back several years.

Child Pornography Collector

20. According to my consultation with other agents, I know that individuals who collect child pornography are sexually attracted to children, and their sexual arousal patterns and erotic imagery focus, in part or in whole, on children.
- a. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences, including children.
 - b. Child pornography collectors express their attraction to children through the collection of sexually explicit materials involving children as well as other seemingly innocuous material related to children. These individuals may derive sexual gratification from actual physical contact with children as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children.
 - c. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity.
 - d. In addition to child pornography, these individuals are also likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica" which is defined as any material, relating to children, that serves a sexual purpose for a given individual. It is broader and

more encompassing, than child pornography, but at the same time the possession of such corroborative material, depending on the context in which it was found, may be behaviorally consistent with the offender's orientation toward children and indicative of his intent. It includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons, and non-sexually explicit visual images.

21. Child pornography collectors reinforce their fantasies, often by taking progressive, overt steps aiming at turning the fantasy into reality in some or all of the following ways:
 - a. Collecting and organizing their child-related material;
 - b. Masturbating while viewing the child pornography;
 - c. Engaging children, online and elsewhere, in conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community;
 - d. Gravitating to employment, activities and/or relationships which provide access or proximity to children;
 - e. Frequent persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement;
 - f. These are need driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.
22. According to my experience, my consultation with other agents and law enforcement officers and my review of previous investigations, I know:

- a. That child pornography collectors almost always maintain and possess their material in the privacy and security of their homes or some other secure location where it is readily available.
- b. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media.
- c. The collector is aroused while viewing the collection and, acting on that arousal, he often masturbates thereby fueling and reinforcing his attraction to children.
- d. Because the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, the collector rarely, if ever, disposes of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase. For example, the time lapse between the obtaining of child pornography by the suspect and execution of search warrants did not result in the lack of evidence, or destruction of all evidence due to the passage of time. Conversely, the passage of time allowed many suspects the opportunity to obtain, view, and possess additional images of child pornography. It is my experience that even if image files are deleted from a computer, they may be able to be recovered from the system using computer forensic tools.
- e. Individuals who utilize a collection in the seduction of children or to document that seduction treat the materials as prized possessions and are especially unlikely to part with them.
- f. Individuals who have a sexual appetite for child pornography are likely to always have that desire, and that such individuals often molest children as well.

- g. The possession of child pornography should always be viewed as both a violation of the law and possible corroboration of child sexual victimization. In the context of child molestation, child pornography and child erotica may be used in several ways, including the following: to desensitize or lower the inhibitions of children targeted for seduction; to arouse the selected child partner; and to demonstrate the desired sexual acts.
- h. While the collection of child pornography does not tell us what the individual has done or will do, it is the best indicator of what he wants to do.

Overall Background

- 23. The FBI's Innocent Images Unit (IIU) and U.S. Immigration and Customs Enforcement (ICE), as part of a joint initiative, have conducted numerous covert transactions to gain access to commercial websites purporting to offer child pornography.
- 24. Of the hundreds of transactions conducted by the Innocent Images Unit and ICE as part of this initiative, a majority have involved a payment website bearing the name "iWest." Over two hundred different child pornography websites processed their payments through the iWest webpage. These websites, which advertise nude images of minors ranging in age from approximately five to sixteen years old, were active on several different URLs, which would typically not be active for more than a few days at a time. The members URL which would be provided to the purchaser after a successful transaction would typically remain active for a longer period of time. All of the websites accessed by the FBI's Innocent Images Unit and ICE advertising paid access to child pornography, which connected to an iWest payment webpage to complete the transaction, contained images of child pornography. The iWest entity does not appear to exist outside of these child pornography websites.

Details of the Investigation

25. In March 2009, I reviewed a report written by FBI Special Agent (SA) Michael Dzielak. Dzielak's report is summarized in the paragraphs below.
26. In September of 2007, SA Dzielak was contacted by Senior Detective on Special Cases Pavel Dudko, of the High-Tech Crime Department of the Ministry of Internal Affairs in the country of Belarus. Dudko was previously a member of an FBI international task-force focused on combating online crimes against children and child pornography.
27. SA Dudko had received confidential information regarding the activities of a group operating several child pornography websites that exists primarily in Belarus, with some members in the Ukraine and others possibly in Russia.
28. Dudko provided SA Dzielak with an Excel spreadsheet consisting of approximately 33,000 transactions and attempted transactions involving the purchase of subscriptions to child pornography websites conducted by individuals located in the United States. This spreadsheet contains information entered by the purchaser (such as Name, Address, Email Address, and Credit Card Number) as well as the Date, Time, and originating Internet Protocol (IP) address of the purchaser.
29. I reviewed this spreadsheet and noted 6 purchases made by an individual identifying himself as Steven Lepak, using the email address shining_sword83@yahoo.com, from June 4, 2007, to September 1, 2007. For the 6 purchases, Lepak provided an address of 338 5th Street North, Hudson, Wisconsin, a telephone number of 715-808-0104, and utilized a WESTconsin Credit Union (WCU) debit card to make the attempted purchases.
30. A review of Wisconsin Department of Transportation records revealed that Lepak has a Wisconsin Identification card, card number XXXXX3606, which was issued on September 14, 2006. The Wisconsin ID card for Lepak listed 338 5th Street North,

Hudson, Wisconsin as Lepak's residence address.

31. On March 6, 2009, a subpoena was served on WESTconsin Credit Union (WCU), located at 444 Broadway, Menomonie, Wisconsin. On March 13, 2009, I received records from WCU in response to the subpoena. The records revealed that a Steven J. Lepak, date of birth X/X/ 1983, residing at 338 5th Street North, Hudson, Wisconsin, telephone number 715-808-0104, opened a bank account with WCU on September 08, 2006. In addition, at the time of the opening of the bank account Lepak provided a Wisconsin Identification card, card number XXXXX3606, date of issuance September 14, 2006.
32. A review of WESTconsin Credit Union records for Steven Lepak from May, 2007, to February, 2009, revealed the following:
 - On June 5, 2007, WCU Steven Lepak had charges for \$79.95 from "PayPal *Bulletproof" and "Paypal *A1 soft tm," respectively. These charges corresponded to transaction records from the aforementioned spreadsheet, which detailed charges on June 4, 2007, and June 5, 2007, for \$79.95 for account membership to <http://www.freshpics.info/lust>, a child pornography website. Records indicate that Lepak on 2 different days, June 4, 2007 and June 5, 2007, purchased account memberships to the same child pornography website, <http://www.freshpics.info/lust>. For each purchase Lepak was assigned a unique username and password to the website.
 - On July 11, 2007, Steven Lepak had a charge for \$79.95 from "Paypal *Bulletproof." This charge corresponded to transaction records from the aforementioned spreadsheet, which detailed a charge on July 10, 2007 for \$79.95 for account membership to <http://goolge.com>, a child pornography website.
 - On September 01, 2007, Steven Lepak had a charge for \$79.95 from "Paypal *A1

soft tm.” This charge corresponds to transaction records from the aforementioned spreadsheet, which detailed a charge on September 01, 2007, for account membership to <http://underage-home.com>, a child pornography website.

33. A review of WESTconsin Credit Union records as of July 01, 2008, reveal that Steven Lepak is residing at 1629 South 37th Street, Milwaukee, Wisconsin.
34. The aforementioned spreadsheet revealed that on 09/10/2006, Steven Lepak attempted to purchase a 30-day membership to website <http://face.cuteloblog.biz/sexyangels/>, a child pornography website, for \$79.95. The attempt was unsuccessful; however, Lepak provided a residence address of 1629 South 37th Street, Milwaukee, Wisconsin and a Wells Fargo Bank debit card in the name of Steven Lepak.
35. The 4 successful transactions, detailed in paragraph 32 above, were for 30 day subscriptions to child pornography websites. Lepak purchased 2 subscriptions to <http://www.freshpics.info/lust>, and one subscription to <http://goolge.com> and <http://underage-home.com>. Each of these subscriptions cost \$79.95.
36. FBI's New Orleans division conducted an undercover operation that targeted individuals with a predisposition to possess child pornography. The undercover server was advertised as a child pornography website, and this advertisement would be sent to individuals predisposed to visit a child pornography website. On May 23, 2008, the FBI New Orleans division utilized its undercover server to send an email advertising access to child pornography websites/content to shining_sword83@yahoo.com, the email address previously used by Steven Lepak. The email contained the following message:

“New kiddy p0rn site. Free trial membership (no credit card necessary).
-no k1ddy over 12 on our site
-daddy teach daughter about \$ex \$erie\$
-daddy teach son about \$ex \$erie\$
-young girl\$ tied up (S&M)

-young boy\$ tied up (S&M)
-and moer...

Free trial until 13 June. After 13 June, membership will be cheap.

Check out our site.

more stuff here

XXXXXXXXXX/specoffer/:4287/:5free23/ch1ld_p0rn.html"

37. If the individual visited the website, the undercover server would record the individual's IP address and other identifying data. Further, after the predisposed individual accessed the undercover CP website the following message would appear:

"Server busy... Because our new website and free trial memberships, we experience high volumes of traffic.
Wait a few moments and try the site again. If you are still experiencing problems, come back in a day or two and get your free trial membership then.
Sorry for the problem."

38. An individual using the email address shining_sword83@yahoo.com responded to the email (sent to shining_sword83@yahoo.com) and attempted to access the link, /specoffer/:4287/:5free23/ch1ld_p0rn.html, 6 times on May 27, 2008. The undercover server recorded IP address 70.92.254.105 on each occasion.
39. On September 04, 2008, an Administrative Subpoena was issued to Time Warner, the Internet Service Provider responsible for the above-referenced IP address. On October 07, 2008, Time Warner advised that the above-referenced IP address was subscribed to by an individual named Eric Szejna, residing at 1629 South 37th Street, Milwaukee, Wisconsin.
40. On March 09, 2009, an Administrative Subpoena was issued to Yahoo! related to the email address shining_sword83@yahoo.com. On March 12, 2009, Yahoo! advised that this email address was in use by an individual identifying himself as "Mr. Steven Lepak."

Yahoo! also advised that the account had been created on August 11, 2005.

41. On March 16, 2009, another FBI undercover website became active on the internet.
42. The FBI's undercover website is a web page that advertises access to free child pornography. The "home" page of the undercover website describes in detail that free child pornography will be available to view and download once users enter in a password. The following is the advertisement on the home page:

"Welcome to the hidden side of yur soul, where you view the yung and innocent. We have been around since 2002, offering the best of private and series Child Pornography (CP), (hard core/soft core) all fore FREE! All you have to do, enter in the password, and you'll be viewing free CP for days. We move around when we have to...congratulations for finding us. Yur old password won't work, so get the new one and you are IN!!!"

"We offer terabytes of free CP images, pictures, and videos of children, toddlers, and pre-teens; all categorized and easy to find in download folders. WHY FREE? Because you like what you see, then you'll want this... **LIVE STREAMING VIDEO** from Eastern Europe, where **YOU** direct the action. This part NOT free, but well worth it. Yur private series... Credit Card required...24/48 hour notice (setup of your video)...high-speed connection"

"Law Enforcement Note: If you happen to be in Law enforcement, FBI or Interpol and are viewing this website, it's called free speech. There is nothing illegal about this website. Our servers are located in a country that has no Child Pornography laws. Even if you are able to shut us down, we pop up again somewhere else..."

43. Individuals learn of the FBI's undercover website through a personal email sent from the undercover agent. Only individuals who have previously attempted to access or purchase child pornography through chat rooms, websites, newsgroups, or other online child pornography forums, receive these email advertisements. The email addresses of these individuals are obtained through other child pornography investigations. Recipients of the email advertisements may delete the email without accessing the website.
44. Individuals who receive this email advertisement and want to access the webpage may do so in one of three ways. An individual may click on the hyperlink provided in the email advertisement, or cut and paste the uniform resource locator (URL) into their web

browser, or type the URL in their web browser.

45. Each recipient of the FBI's undercover website advertisement email is sent a unique password. Once an individual accesses the undercover website home page, he or she has two options: one, close the website without attempting to download or access the free child pornography, or two, enter his or her unique password to gain entry and access to the second page of the website. There is no indication on the website home page that any adult pornography or anything other than child pornography will be made available through this website.

46. After accessing the FBI's undercover website with his or her unique password, the individual is taken to the "second" page of the undercover website. The second page lists approximately 35 free child pornography videos available to view and/or download. Each video, described in graphic detail, has a download "button" that offers access to a free, one-minute sample. The following is the list of videos that are available:

FREE 1 MINUTE SAMPLES

01.	3 10-11 y.o. Kenyan girls playing together. Masturbation, petting, lesbians.	70 mins	DOWNLOAD
02.	3 3-4 y.o. girls and man. Masturbation, petting, sucking.	100 mins	DOWNLOAD
03.	Full version of known video. 3 10-12 y.o. girls and man. Masturbation, petting, fingering, pissing, sucking, lesbians.	72 mins	DOWNLOAD
04.	Full version of known video. 9-10 y.o. girl and man. Masturbation, petting, fingering, pissing, sucking, sex simulation.	71 mins	DOWNLOAD
06.	7-9 y.o. latino girls and man. Masturbation, petting, sucking, fingering, pissing, sex simulation.	66 mins	DOWNLOAD
07.	8-11 y.o. girls and boys and man. Masturbation, petting, sucking, fingering, pissing, sex simulation, anal. (No Sound)	62 mins	DOWNLOAD
08.	8 y.o. girl and man + 3 13 y.o. girls and man. Masturbation, petting, fingering. (Grainy graphics)	71 mins	DOWNLOAD
09.	Japanese origin video. 3 5-6 y.o. girls and man.	69 mins	DOWNLOAD

	Masturbation, petting, sucking, fingering, pissing, sex simulation.		
10_1.	2 9 y.o. girls and dad and dog. Masturbation, petting, sucking, fingering, pissing, sex simulation, anal. PART ONE. forced	71 mins	DOWNLOAD
10_2.	PART TWO of this video.	72 mins	DOWNLOAD
11.	7-9 y.o. Eastern European girls and man. Masturbation, petting, sucking, fingering, anal, sex simulation.	59 mins	DOWNLOAD
12.	newborn baby girls and euro man. Masturbation, petting, sucking, fingering, anal, sex simulation.	68 mins	DOWNLOAD
13.	3 13-14 y.o. Romanian girls and man. Masturbation, petting, sucking, sex, lesbos.	54 mins	DOWNLOAD
14.	12-13 y.o. girl, man and woman. Masturbation, petting, lesbos, sucking, vaginal and anal penetration, fingering, sex simulation.	11 mins	DOWNLOAD
15.	CP Mix - short clips from different videos. 7-12 y.o. girls and boys.	53 mins	DOWNLOAD
16.	9-11 y.o. girls, 15 y.o. boy and man. Masturbation, petting, sucking, fingering, anal, sex simulation.	97 mins	DOWNLOAD
17.	13 y.o. girl and man. Masturbation, petting, sucking.	73 mins	DOWNLOAD
18.	7-9 y.o. girls and 8 y.o. boy. Masturbation, petting, fingering, sex simulation.	95 mins	DOWNLOAD
19.	12 and 14 y.o. girls and man. Masturbation, petting, lesbos, sucking, vaginal and anal penetration, fingering.	55 mins	DOWNLOAD
20.	1-4 y.o. black boys. Masturbation, petting, sucking, fingering.	35 mins	DOWNLOAD
21.	9 y.o. girl and man. Masturbation, petting, pissing, sex simulation, zoo.	48 mins	DOWNLOAD
22.	5 6-14 y.o. South African girls and man. Masturbation, petting, pissing, lesbos, vaginal penetration, fingering, sex simulation.	9 mins	DOWNLOAD
23.	11 and 14 y.o. girls, man and woman. Masturbation, petting, lesbos, vaginal and anal penetration, fingering, sex.	50 mins	DOWNLOAD
24.	4 11-14 y.o. girls. Masturbation, petting, lesbos, vaginal penetration, fingering.	44 mins	DOWNLOAD
25.	6 y.o. Jewish girl and father. Masturbation, petting, sex simulation.	3 mins	DOWNLOAD

26.	8 and 14 y.o. girls and man. Masturbation, petting, lesbos, vaginal and anal penetration, fingering, pissing, sex simulation.	10 mins	DOWNLOAD
27.	9 and 12 y.o. asian girls and 16 y.o. boy. Sucking, masturbation, petting, vaginal penetration, fingering, pissing, sex simulation.	57 mins	DOWNLOAD
28.	2 12 y.o. asian girls and 16 y.o. boy. Sucking, masturbation, petting, vaginal penetration, fingering, pissing, sex simulation.	9 mins	DOWNLOAD
29.	7 y.o. Somali girl and soldier. Masturbation, petting,	51 mins	DOWNLOAD
30.	9 and 12 y.o. latin girls and boy. Masturbation, petting, sucking, vaginal and anal penetration, fingering, sex simulation.	47 mins	DOWNLOAD
31.	12 y.o. girl, 11 y.o. boy and father. Masturbation, petting, sucking, fingering, sex simulation.	22 mins	DOWNLOAD
32.	Muslim 5 y.o girl/boy. FORced vaginal and anal penetration, fingering, sex simulation.	6 mins	DOWNLOAD
33.	10 y.o. girl and man. Masturbation, petting, fingering, anal, sex simulation. BONDAGE and PAIN	26 mins	DOWNLOAD
34.	Same man and 3 7-9 y.o. girls. Masturbation, petting, fingering, vaginal and anal penetration, sex simulation.	51 mins	DOWNLOAD
35.	12 y.o. asian girl and man. Masturbation, petting, pissing, fingering, sucking.	28 mins	DOWNLOAD

47. When the user clicks on the download "button," their web browser opens another webpage that appears to start the child pornography video download. After several seconds the video download appears to slow and then stop. Once the individual clicks the download "button," their IP address, video sample number, the number of downloads attempted and other identifying information is recorded. No child pornography is actually made available to any individuals through the FBI's undercover website.

48. On March 27, 2009, the FBI Innocent Images Unit utilized its undercover server to send an email advertising access to child pornography websites/content to

shining_sword83@yahoo.com.

49. On March 27, 2009, between 18:23 to 19:00 EDT, an individual utilizing the IP address 70.92.248.2, used the unique password provided to shining_sword83@yahoo.com to access the second page on the FBI's undercover websites home page. The individual utilizing this IP address and unique password identifier then clicked on the link for free 1 minute samples of videos numbered 1, 3, 4, and 35. These videos are described in paragraph 46 and all advertised child pornography.

50. Utilizing commercially available software, the IP address 70.92.248.2 was determined to be assigned to ISP Time Warner/Road Runner. On May 04, 2009, an administrative subpoena was sent to Road Runner for basic subscriber information and physical address for the individual utilizing IP address 70.92.248.2 on March 27, 2009 between 18:23:10 to 19:00:23 EDT.

51. On June 15, 2009, the Time Warner/Road Runner advised that the above-referenced IP address was subscribed to by an individual named Eric Szejna, residing at 1629 South 37th Street, Milwaukee, Wisconsin.

52. A search of the public records database, ChoicePoint, on August 19, 2009 indicated that four individuals, Eric Szejna, DOB X/X/1964; Andrew Szejna, DOB X/X/1986; Sandra Lepak-Szejna, DOB X/X/1961, and Steven J. Lepak currently reside at 1629 South 37th Street, Milwaukee, Wisconsin.

Seizure of Computer and Electronic Evidence

53. Based upon my experience, I know that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripheral equipment) to be imaged and searched later by a qualified computer specialist in a laboratory or other controlled environment. This requirement is due to the following:

- a. Technical requirements. Images or backups of computer data need to be restored to a separate computer and verified to ensure that the files restore or copy properly. Additionally, evidence may be encrypted, password protected, or may be in a format that could result in additional evidence being overwritten and/or destroyed electronically should an attempt be made to examine the electronic evidence on site.
 - b. The volume and nature of electronic evidence. A seemingly small media storage device can store the equivalent of thousands of pages of information or more. It may be impractical to attempt data analysis on site.
54. Based upon my experience, I know that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects:
- a. The objects themselves may be instrumentalities used to commit the crime;
 - b. The objects may have been used to collect and store information about crimes (in the form of electronic data).

Application

55. Based on the facts as stated in this affidavit, there is probable cause to believe that evidence of the stated violations is located at the residence located at 1629 South 37th Street, Milwaukee, Wisconsin.
56. I respectfully request that the Court issue a search warrant for the items listed in "Attachment A" which is attached to this affidavit.

Place to be Searched

57. The residence at 1629 South 37th Street, Milwaukee, Wisconsin, is more particularly described as follows: A two-story residence, the lower half of the residence contains while

siding with maroon trim and the upper half contains maroon siding with white trim. The address "1629" is affixed to the mail box near the front door of the residence. In addition, there is a detached two-car garage with light colored siding and a red garage door.